REMARKS

This responds to the Office Action mailed on February 14, 2005. Reconsideration is respectfully requested. By this amendment, claims 1 – 23 are amended, no claims are canceled, and no claims are added; as a result, claims 1 – 23 remain pending in this application.

§112 Rejection of the Claims

Claims 9 was rejected under 35 USC § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. The Examiner states that the phrase "Blakley-Shamir" is unclear. Claim 9 has been amended to recite that the key-shares are generated from the decryption key using a key-splitting technique. In view of this, Applicant submits that the rejection of claim 9 under 35 USC § 112, second paragraph has been overcome.

§103 Rejection of the Claims

Claims 1-4, 6, 8, 10-17 and 19-20 were rejected under 35 USC § 103(a) as being unpatentable over Downs et al. (U.S. 6,226,618) and further in view of Hardjono (U.S. 6,182,214). Applicant's claim 1, for example, is directed to secure distribution of content to a wireless communication device and to secure usage of the content in the wireless device. A user's private decryption key is split into several key-shares and the key-shares are distributed in various network elements. For example, as recited in some claims, a financial server and a security server may each hold a key-shares, and the user device may hold the third key-share. One of the key-shares, (e.g., the third key-share) is stored in the user's wireless device beforehand (i.e., pre-stored before the wireless device requests the content). In this way, the third key-share does not have to be provided over a wireless link. Since the first and second key-shares cannot be used without the third key-share, there is no reason to encrypt the first and second key-shares when sending them to the user's wireless device. This technique allows

content to be encrypted anytime, including *after* the user already has the third key-share stored in the wireless device, allowing only the user to decrypt when all key-shares are combined.

As recited in Applicant's claim 1, the third key-share is pre-stored in the wireless communication device. The wireless device is provided the first key-share in response to a request for content, and the wireless devices is provided the second key-share when the credit is verified. The first and second key-shares are combined with the third key-share that is pre-stored in the wireless communication device to decrypt the content. Claim 1 also recites that the first, second and third key-shares are associated with the user (i.e., rather than the content) and comprise a private decryption key of the user.

Claim 15, for example, further recites that the first and second of the key-shares are transferred over a wireless communication link to the wireless device and that the third key-share is pre-stored in the wireless communication device prior to the user generating the request for the content and prior to a security server sending the content to the wireless communication device.

Claim 7, as amended, recites that the third key-share is pre-stored in a subscriber identity module (SIM) associated with the user and that a fourth of the key-shares is pre-stored in the wireless communication device and associated with a security processor of the wireless communication device. Claim 7 also recites that the security processor combines the first, second, third and fourth key-shares to generate the decryption key and decrypt the encrypted content.

Downs, on the other hand, provides many users with a whole (i.e., not split) decryption key for decrypting content that is provided to many users. In Downs, the decryption key is associated with the content and not the user. This makes it impossible for Downs to pre-store decryption keys for content in user devices. One problem with Downs is that the entire decryption key is provided to the users *after* the clearinghouse 105 validates the request. Therefore, the encryption key must be secured or encrypted so that only an authorized user can retrieve it. (See Downs col. 10, lines 50 – 67). Applicant's claims do not have this problem. Applicant's claims, on the other hand, do not need to encrypt a decryption key because less than all key-shares are transmitted over the wireless link to the user device. Applicant's wireless communication device already has one or more key-shares pre-stored therein, so there is really no need for the key-shares to be encrypted before transmission. In Applicant's claims, the

decryption key and the key-shares are pre-generated prior to the user ever requesting the content. The content, however, may be pre-encrypted or post encrypted with an associated encryption key, which may be a public encryption key.

As can be seen, the use of asymmetric keys (i.e., public and private key pairs) to encrypt content is not suitable for use in Downs because in Downs, the encrypted content must be usable by many users. Downs, however, discloses the use of public and private key pairs to encrypt the *symmetric* encryption/decryption key that is used to encrypt the content (see Downs Abstract), but this is unlike Applicant's claims which do not need to secure the key-shares sent to the user device.

As recited in some of Applicant's amended claims, Applicant's private decryption key is associated with the user or the user device which only allows the content to be decrypted with the particular user device having the proper key-share stored therein. Accordingly, the content that is sent to Applicant's user device is encrypted with an encryption key (such as a public encryption key) associated with user's decryption key. In this way, the security server, as recited in claims 4, and 5 for example, and the finance server as recited in claim 8 for example, may store key-shares associated with individual users so they know which key-share to send to a particular user. Applicant finds no such teaching in any of the cited art.

Applicant further finds no teaching, suggestion or motivate in Downs of verifying credit of user prior to sending the user a key-share, as recited in Applicants claim 1. In Downs, the clearinghouse (a licensing authority) only validates that integrity and authenticity of the request, and verifies that the request was authorized by either a content provider of a digital content store (see Downs, column 10, lines 50 – 59). There is no user credit verification in Downs. Downs is concerned with the integrity and authenticity of the request itself. Downs states that the clearinghouse can provide billing, however there is no credit verification *prior to* providing either content or a decryption key or key-share (see Downs, column 11, lines 16 – 28).

Applicant further submits that the teachings in Downs are not suitable for use of key-splitting or the use of key shares because in Downs, only one entity (i.e., the clearinghouse) controls the final distribution and security of the content. Furthermore, in Downs, each user would have the same decryption key allowing any user to decrypt the content. This application of

Downs *teaches away* from Applicant's claimed invention which only allows a user with the user's key share stored within the user's device to decrypt and use the content.

Applicant's claim 16, as amended, is directed to a processing system that includes a security processor portion to combine first, second and third key-shares to generate a decryption key to decrypt content for the processing system. The security processor portion includes a monitor for usage of the content constructed and is arranged to purge at least one of the key-shares when the usage exceeds a measurement parameter. The processing system also includes a communications processor portion to receive decrypted content from the security processor portion and providing decrypted content for playing on the wireless communication device. As further recited in claim 16, the wireless communication device has the third key-share pre-stored therein, and receives the first key-share and the second key-share over a wireless link in response to a request for content and a verification of a user's credit.

Applicant's claim 21, as amended, is directed to a wireless communication device that includes a processor area to store first key-share, and a module receiving area to receive a subscriber identity module (SIM) which has a second key-share stored therein. The wireless communication device also includes an RF interface to receive a third key-share and encrypted content over a wireless communication link in response to a request for content and verification of a user's credit. As recited in claim 21, the first, second and third key-shares are combined in the processor area to decrypt the encrypted content and monitor playing of the decrypted content against measurement parameters. As further recited in claim 21, the first, second and third key-shares are associated with the user and comprise a private decryption key of the user. As further recited in claim 21, the first key-share is pre-stored in the processor area and the second-key-share is stored in the SIM prior to the device generating the request for the content and prior to a security server sending the content and the third-key-share to the wireless communication device.

In view of the above, Applicant submits that the recitations of claims 1, 16 and 21 are not taught, suggested or motivated by Downs, either separately or in combination with other cited references and that claims 1, 16 and 21 are allowable over the cited art. Applicant further submits that claims 2 – 15, 17 – 20, 22 and 23 are allowable at least because of their dependency on either claim 1, 16 or 21.

Hardjono is cited by the Examiner for teaching the use of key-shares. Applicant submits that Hardjono teaches distributing a secret is parts to multiple clients over a multicast network. A client can reconstruct the secret when a sufficient number of shares is received (see Hardjono column 3, lines 29 – 42, and column 3 line 64 through column 4 line 9). As discussed above, Applicant submits that the teachings in Downs are not suitable for use of split keys or key-sharing and therefore there would be no motivation to combine Downs with Hardjono. Applicant further submits that the splitting of a secret, as taught in Hardjono, teaches away from Applicant's claims when combined with Downs, because Downs is concerned with secure distribution of content to many users, rather that controlling use of content by an individual user.

Applicant further submits that claims 1, 16 and 21 further distinguish over the cited art because they concern wireless communication devices. Downs electronic content delivery system is applicable to *wireline networked communications* (see Downs column 1, lines 52 – 57). The end user devices 109 of Downs are wireline devices, such as set top boxes and Internet Appliances (see Downs column 11, lines 30 – 34).

Applicant further submits that claims 14, 17 and 22 further distinguish over the cited art by reciting the use of an authentication code associated with the measurement parameters. The security processor purges at least one of the key-shares when the authentication code fails to authenticate. Applicant finds no teaching, suggestion or motivation in Downs or Hardjono of using an authentication code in this way.

Applicants claims 2, 11, 14, 16, 17, 19 and 22 further distinguish over the cited art by reciting that at least one of the key-shares is purged when, for example, usage of the content exceeds a measurement parameter. In Downs, *there are no explicit or implicit teachings* to purge a decryption key in the end user device. According to Downs, "The end user device ... processes watermarks every time the Digital Content is copied or played; manages the number of copies made (or deletion of a copy) in accordance with the ... usage conditions." In Downs, there are no key-shares to purge. Furthermore, in Downs the use of the decryption key may simply be restricted based on the processed watermarks, so there is no requirement to purge the key.

In summary, Downs does not teach, suggest or motivate, either separately, or in combination with other cited references:

1) The pre-storing of key-shares in a wireless communication device (Downs sends an *entire* decryption key *after* content is encrypted);

2) The performance of a credit verification before transmitting a key-share (Downs does not perform any credit verification whatsoever, particularly *before* sending the content or a decryption key);

3) The transmission of content and less than all key-shares over wireless links (Downs must encrypt his decryption key because the entire key is sent);

4) The storage of separate key-shares in a finance server and a security server (Downs does not use key-shares and only one entity, the clearinghouse, sends the whole decryption key);

5) The association of a decryption key for decrypting content with an individual user (In Downs, the same decryption key is sent to all users);

6) The use of asymmetric cryptography for securing content (Downs uses a symmetric cryptography to encrypt and decrypt the content);

7) The use of a separate authentication code along with measurement parameters; and

8) The purging of a key-share from the end-user device.

In view of the above, Applicant submits that the rejection of claims 1- 23 under 35 USC § 103(a) has been overcome.

Claim 5 was also rejected under 35 USC § 103(a) as being unpatentable over Downs et al. and Hardjono and further in view of Howard et al. (U.S. 2002/0069365). Claims 7, 18 and 21-23 were also rejected under 35 USC § 103(a) as being unpatentable over Downs et al. and Hardjono and further in view of Johnston (U.S. 6,373,946). Claim 9 was also rejected under 35 USC § 103(a) as being unpatentable over Downs et al. and Hardjono and further in view of Schneier (Applied Cryptography, 1996, pp. 71-72). In view of the discussion above with regard to Downs and Hardjono, Applicant submits that the further rejection of claims 5, 7, 9, 18 and 21 – 23 has been overcome.

Conclusion

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicants' attorney, Greg Gorrie at (480) 659-3314, or Applicants' below-named representative to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

ERNEST E. WOODWARD

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
Attorneys for Intel Corporation
P.O. Box 2938
Minneapolis, Minnesota 55402
(612) 349-9592

Date May 16, 2005 By Ann M. McCrackin
Ann M. McCrackin
Reg. No. 42,858

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: MS Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 16 day of May 2005.

John D. Gustav-Wrathall
Name

John D. Gustav-Wrathall
Signature